



# Health Information Privacy

**National Quality Monitoring Contract (NQMC)  
Pre-Proposal Conference**

**Paul Bley, Office of General Counsel  
TRICARE Management Activity**

*May 2003*

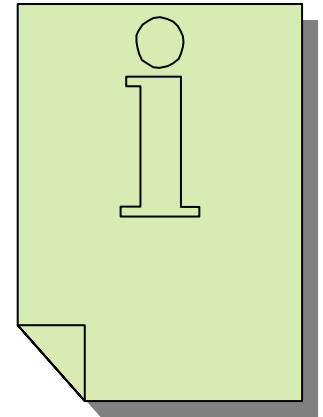
# [ Presentation Objectives ]

- Provide an overview of the HIPAA legislation
- Explain key HIPAA Privacy components
- Describe HIPAA Privacy impacts on the patient healthcare experience
- Provide an overview of the Automated Data Processing (ADP) clearance process



# [ Federal Privacy Milestones ]

- Freedom of Information Act
  - Right of access to federal agency records
- Privacy Act of 1974
  - Controls over how the executive branch agencies of the federal government gather, maintain, and disseminate personal information



# [ The Latest Privacy Stride ]

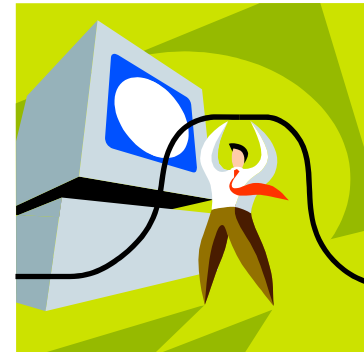
## Health Insurance Portability and Accountability Act (HIPAA)

Public Law 104-191 enacted August 21, 1996

- Improve portability & continuity of health insurance coverage
- Improve access to long term care services and coverage
- Simplify the administration of health care

# [ HIPAA Rules ]

- Transactions and Code Sets
- Privacy
- Security
- Identifiers



# [ From the Patient's Viewpoint ]

HIPAA's greatest impact on the patient's healthcare experience is the Privacy Rule

Compliance Date:  
April 14, 2003



HIPAA Privacy

# What Organizations are Affected?

Healthcare providers who transmit health information in electronic transactions

## HIPAA ENTITY

## MHS ENTITY

Health plans       TRICARE Health Plan

Healthcare clearinghouses       Companies that perform electronic billing on behalf of MTFs

Business associates       Managed care support contractors

# What Information is Protected?

## Protected Health Information (PHI)

- Individually identifiable health information (including demographics) in electronic, paper or oral medium
- Held by health plans, healthcare providers or their business associates

*Any health information that identifies you as you*



# HIPAA Privacy **Key Concepts**

- Treatment, Payment & Healthcare Operations (TPO)
- Minimum Necessary
- Patient Rights
- Notice of Privacy Practices
- HIPAA Privacy Officers



# Treatment, Payment and Healthcare Operations

HIPAA allows the use and disclosure of PHI for treatment, payment & healthcare operations (TPO) without the patient's permission.

*HIPAA Privacy is not meant to impede the provision of quality care*

# HIPAA Privacy **Treatment**

- Provision of care
- Coordination or management of healthcare and related services
- Consultations between providers
- Referral of a patient from one provider to another



# HIPAA Privacy **Payment**

- Obtaining premiums
- Reimbursement
- Eligibility and coverage determinations
- Billing and claims management
- Utilization review activities



# HIPAA Privacy Healthcare Operations

- Quality assurance
- Health improvement
- Education and training
- Legal services
- Medical review
- Business planning and development
- Management and general administrative activities



# Minimum Necessary Principle

- All uses and disclosures of information are limited by the 'need-to-know' standard
- Only the amount of information reasonably necessary to achieve the purpose of the release is permitted

# Patient Rights

Patients have a right to:

- A written notice of information practices
- Request to access, inspect and obtain a copy of their PHI
- Request an accounting of disclosures
- Request amendment of records
- Request restrictions on uses and disclosures of their PHI
- Accommodation of reasonable alternate communications requests
- Complain to the organization (MHS) or Department of Health and Human Services

# Exercising Patient Rights

- Unless covered by other privacy legislation, these rights became effective April 14, 2003
- Complaints may be made to the MTF HIPAA Privacy Officer, TMA HIPAA Privacy Officer or Department of Health and Human Services
- Information requests must be made by the person whose PHI is impacted, the appointed caregiver, or other authorized representative.
- All information requests must be made in writing to the local MTF HIPAA Privacy Officer where the patient obtained care, or where the PHI is located.



HIPAA Privacy

# Notice of Privacy Practices

Explains

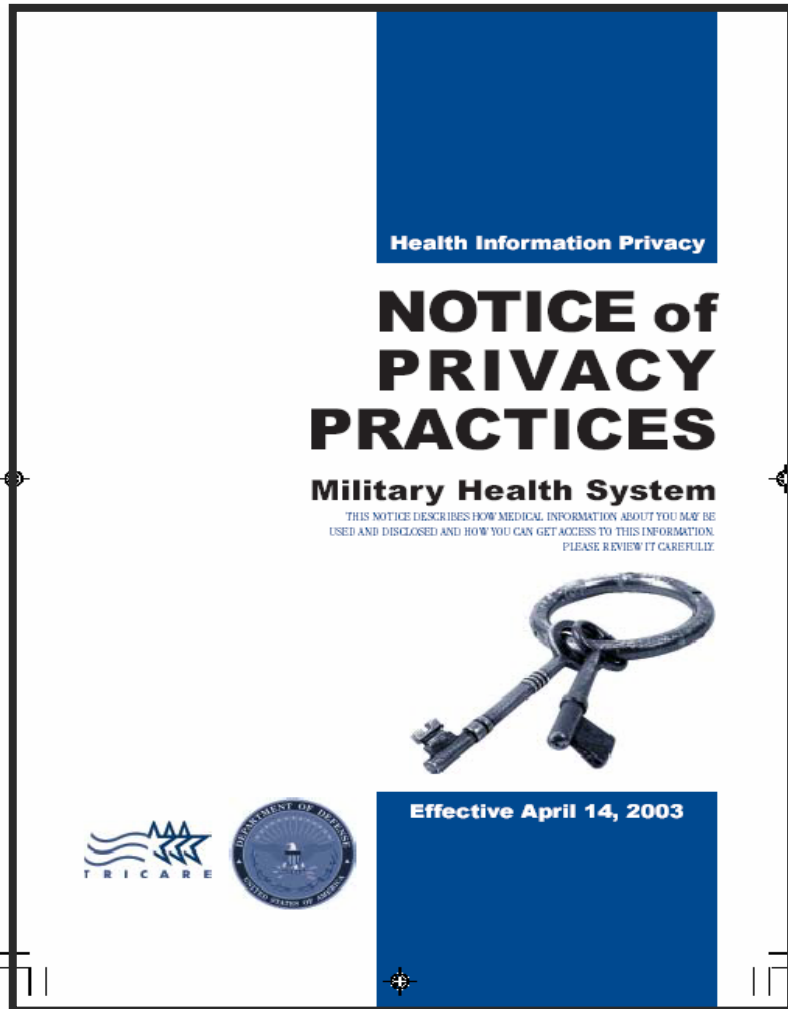
- MHS duty to beneficiaries to protect health information
- How the MHS may use and disclose health information
- Patients' rights
- Patient complaint procedures
- Contact information

# **What You Need To Know About The Notice**

- The Notices of Privacy Practices have been mailed to sponsor households.
- Beneficiaries will acknowledge receipt of the Notice by signing a medical record jacket label when they visit their MTF. No action is required by the beneficiary until that time.
- The Notice became effective on the HIPAA Privacy Rule compliance date of April 14, 2003.

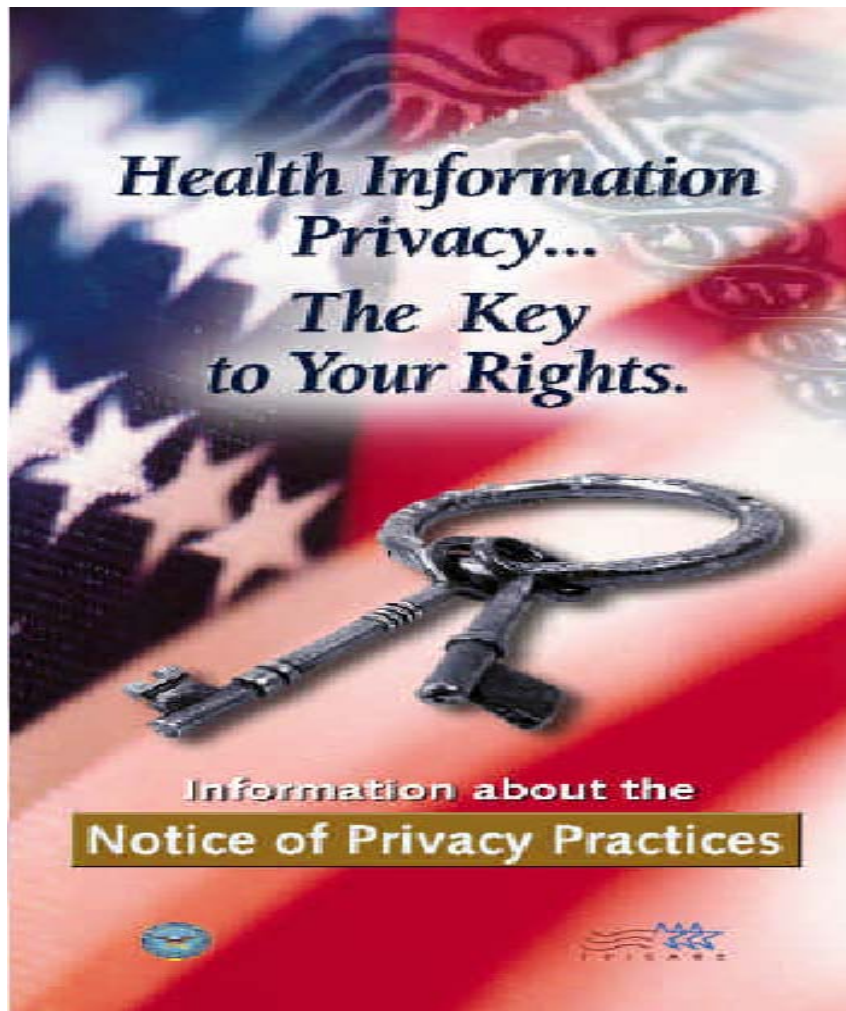
HIPAA Privacy

# Getting the Notice



- Mailed to sponsor households
- Available at [www.tricare.osd.mil/hipaa](http://www.tricare.osd.mil/hipaa) in multiple formats and languages
- Beneficiaries may direct questions to 1-888-DODHIPA , or [hipaamail@tma.osd.mil](mailto:hipaamail@tma.osd.mil)

# HIPAA Privacy Beneficiary Brochure



- Explains the purpose of the Notice of Privacy Practices
- Available at MTFs

HIPAA Privacy

# MTF HIPAA Privacy Officers



- Assigned at every MTF
- Available to answer specific questions
- Address PHI requests and patient complaints

ADP Process

# Contract Requirement - ADP

## NQMC Proposal

C-6.3.7. Information Systems (IS)/Networks Personnel Security. The NQMC shall achieve the same level of trustworthiness of personnel who have access to IS/Networks involved in the operation of its systems of records as required for Government personnel requiring similar access to DoD information technology systems and networks containing sensitive information (SI) (See Appendix 6, DoD 5200.2-R, June 2002 (draft) Positions Requiring Access to DoD Information Technology (IT) Systems and Networks, found on the TRICARE web site at [www.tricare.osd.mil/tmis\\_new/ia.htm](http://www.tricare.osd.mil/tmis_new/ia.htm) ).



# Clearance Levels - I

- Privileged access to networks and information systems, system security and network defense systems, or to system resources
- Duties broad in scope and authority and provide access to the U.S. Government, DoD, or Component mission critical systems
- Potential exists for exceptionally serious adverse impact on U.S. Government, DoD, Component or private sector information and/or operations, with worldwide or government-wide effects
- May be responsible for unsupervised funds disbursements or transfers or financial transactions totaling over \$10M per year
- Clearance valid for 5 years

# Clearance Levels - II

- Limited privileged access, but duties of considerable importance to the DoD or DoD Component mission
- Under the supervision of an individual in a higher trust position (IT-I)
- Potential for moderate to serious adverse impact on DoD or Component information or operations
- Responsible for monitored/audited funds disbursements or transfers or financial transactions totaling less than \$10M per year
- Clearance valid for 10 years



# Clearance Levels - III

- Non-privileged access to one or more DoD information systems/applications.
- Can receive, enter and/or modify information in an information system/application or database to which they are authorized access. Access only to that data/information and those applications/networks which are explicitly authorized or has need-to-know and cannot alter those or other users' authorizations.
- Potential exists for limited adverse impact on DoD, Component or unit information or operations.
- May be responsible for financial operations subject to routine supervision or approval, but has no funds disbursement or transfer capabilities.
- Clearance valid for 15 years

ADP Process

# Contract Requirement - SI

## NQMC Proposal

C-6.3.7. All NQMC employees with access to sensitive information (SI) that is maintained in NQMC owned and operated IT systems that have no interconnection (including data feeds) with Government IT systems or networks, shall complete the appropriate background check for IT-III level personnel comparable to that described in the referenced Appendix 6 to DoD 5200.2-R unless the NQMC proposes, and the Contracting Officer approves, other alternative safeguards appropriate to mitigate the risks associated with the loss/misuse or unauthorized access to or modification of the SI.



ADP Process

# **Sensitive Information Access**

Persons with access to sensitive information, but without access to DoD applications must obtain Level III ADP clearance or an acceptable agreement with the Contracting Officer.

# Alternatives Safeguards

*“ ... alternative safeguards appropriate to mitigate the risks associated with the loss/misuse or unauthorized access to or modification of the SI.”*

Things to consider when developing ‘alternative safeguards’:

- Intention is for the contractor to certify the trustworthiness of the employee
- Innovation encouraged
- Alternative must be equal to the level of confidence provided by a background check
- Options could include bonding of employees or vouchering of applicants

# Process Upon Award of Contract

1. Contact TMA to obtain TMA's Submitting Office Number (SON).
2. Submit ***PIPS form 12*** to OPM to obtain your organization's SON.
3. When received from OPM provide your SON along with your organization's POC information, and contract number to TMA.
4. Submit ***SF 85P Questionnaire for Public Trust Positions*** to OPM. Form requires original signature of the employee and the contractor's Security Officer.



# Process Upon Award of Contract

5. Notify TMA of completed submissions including names of personnel and social security numbers.
6. When TMA receives the confirmation submittal order from OPM, a letter will be forwarded to the contractor's POC indicating approval of interim access pending final investigation.
7. Notification of approvals and denials will be communicated in writing.



# ADP Process **Resources**

To download SF 85P Questionnaire for Public Trust Positions, go to

[www.opm.gov/forms/pdfimage/SF0085p.pdf](http://www.opm.gov/forms/pdfimage/SF0085p.pdf)

To obtain PIPS form 12, contact OPM at  
US Office of Personnel Management  
Investigations Service  
P.O. Box 618  
Boyers, PA 16018  
724-794-5612  
[www.opm.gov](http://www.opm.gov)

[

]

**Questions?**



A horizontal blue line spans the width of the slide. A large black left square bracket is positioned on the left side of the line, and a large red right square bracket is positioned on the right side of the line.

**Mr. Thomas Fuller**